



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002344440 A**(43) Date of publication of application: **29.11.02**

(51) Int. Cl.
H04L 9/08
G11B 20/10
H04L 9/16
H04N 5/93
H04N 7/173

(21) Application number: **2001150968**(22) Date of filing: **21.05.01**(71) Applicant: **TOSHIBA CORP**(72) Inventor: **OGAMI AKIHIRO**

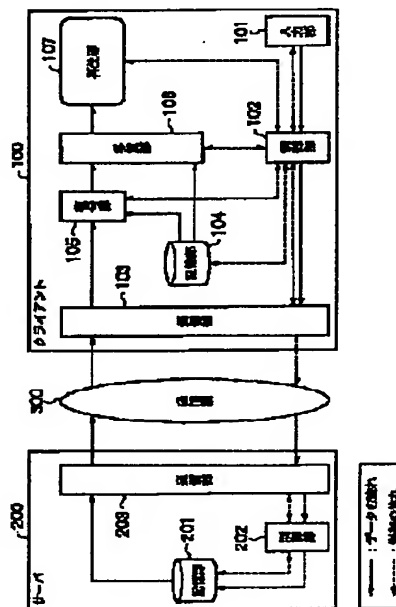
(54) **DATA-REPRODUCING DEVICE AND DATA
 REPRODUCING METHOD, DATA REPRODUCING
 PROGRAM AND VIDEO-ON-DEMAND SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a data reproducing device, capable of instantaneously starting the reproduction of digital data by shortening an access time, since the reproduction of digital data is instructed by a user, until the reproduction of digital data is actually started.

SOLUTION: The preceding data part of digital data obtained, by converting information such as characters, voices, static images, and moving images into digital signals is non-enciphered, and only the subsequent data part is enciphered, and the digital data are distributed to a client. When the reproduction of the digital data is instructed, a client requests key data for solving the cryptograph to a server and reproduces the leading data part of the digital data in parallel.

COPYRIGHT: (C)2003,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-344440

(P2002-344440A)

(43) 公開日 平成14年11月29日 (2002. 11. 29)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 L 9/08		G 1 1 B 20/10	H 5 C 0 5 3
G 1 1 B 20/10			3 2 1 Z 5 C 0 6 4
	3 2 1	H 0 4 N 7/173	6 3 0 5 D 0 4 4
H 0 4 L 9/16		H 0 4 L 9/00	6 0 1 B 5 J 1 0 4
H 0 4 N 5/93		H 0 4 N 5/93	E

審査請求 未請求 請求項の数15 O L (全 12 頁) 最終頁に続く

(21) 出願番号 特願2001-150968(P2001-150968)

(22) 出願日 平成13年5月21日 (2001. 5. 21)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 大上 晃弘

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝マイクロエレクトロニクスセンター内

(74) 代理人 100083806

弁理士 三好 秀和 (外7名)

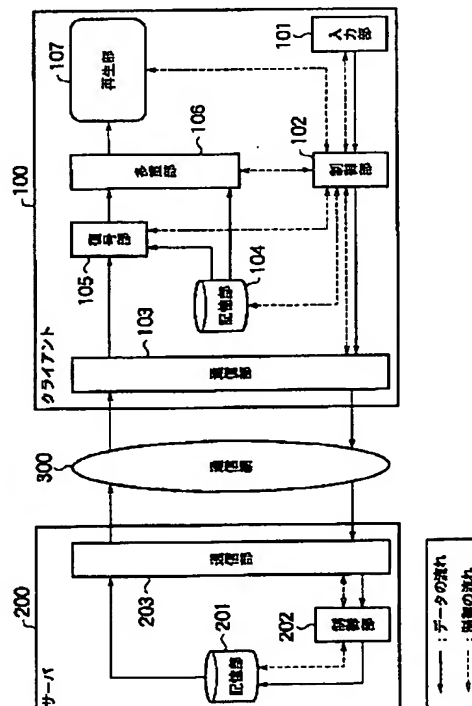
最終頁に続く

(54) 【発明の名称】 データ再生装置、データ再生方法、データ再生プログラム、およびビデオ・オン・デマンド・システム

(57) 【要約】

【課題】 利用者が再生の指示をしてから実際にデジタルデータの再生が開始されるまでのアクセス時間を短縮し、即座にデジタルデータの再生を開始することのできるデータ再生装置を提供することを提供すること。

【解決手段】 文字、音声、静止画像、動画像、等々の情報をデジタル信号化したデジタルデータの、先行データ部分は非暗号とし、後続データ部分にのみ暗号化を施して、クライアントに配布しておき、クライアントは、再生指示がなされたら、サーバへの暗号を解くための鍵データの要求とデジタルデータの先行データ部分の再生とを並行して行うことによる。



【特許請求の範囲】

【請求項 1】 先頭から所定の長さ分の先行データ部分は非暗号化され、先行データ以降の後続データ部分は所定の暗号方式により暗号化されたデジタルデータを記憶する記憶部と、

前記記憶部に記憶されたデジタルデータの再生の指示を受け付ける入力部と、

前記暗号方式による暗号を復号するための鍵データをサーバに要求し、該サーバから送られてくる前記鍵データを受信する通信部と、

前記通信部が受信した前記鍵データにより、前記記憶部に記憶されたデジタルデータの後続データ部分を復号する復号部と、

前記デジタルデータを再生する再生部と、

前記各部を制御する制御部とを有し、

前記入力部により再生指示がなされたら、前記通信部によるサーバへの鍵データの要求と、前記再生部による前記デジタルデータの先行データ部分の再生とを並行して行い、

前記通信部が受信した鍵データを用いて、前記復号部により前記デジタルデータの後続データ部分の暗号を復号化し、

前記デジタルデータの先行データ部分の再生後に、前記復号部により復号化した前記デジタルデータの後続データ部分を前記再生部により再生することを特徴とするデータ再生装置。

【請求項 2】 デジタルデータの先頭から所定の長さ分の非暗号化された先行データ部分を記憶する記憶部と、前記デジタルデータの再生の指示を受け付ける入力部と、

前記先行データ部分以降の所定の暗号方式により暗号化された後続データ部分と前記暗号方式による暗号を復号するための鍵データとをサーバに要求し、該サーバから送られてくる前記鍵データと前記後続データ部分とを受信する通信部と、

前記通信部が受信した前記鍵データにより、前記デジタルデータの後続データ部分を復号する復号部と、

前記デジタルデータを再生する再生部と、

前記各部を制御する制御部とを有し、

前記入力部により再生指示がなされたら、前記通信部によるサーバへの鍵データ及び前記デジタルデータの後続データ部分の要求と、前記再生部による前記デジタルデータの先行部分の再生とを並行して行い、

前記通信部が受信した鍵データを用いて、受信した前記デジタルデータの後続データ部分の暗号を前記復号部にて復号化し、

前記デジタルデータの先行データ部分の再生後に、前記復号部により復号化した前記デジタルデータの後続データ部分を前記再生部により再生することを特徴とするデータ再生装置。

【請求項 3】 前記データ再生装置は、更に、

前記記憶部に記憶されている前記デジタルデータの先行データ部分に引き続いて、前記復号部にて復号化される前記デジタルデータの後続データ部分を、前記再生部に順次送る多重部を有することを特徴とする請求項 1 ないし請求項 2 のいずれかに記載のデータ再生装置。

【請求項 4】 前記データ再生装置は、更に、

前記記憶部に記憶されている前記デジタルデータの先行データ部分を前記再生部に、後続データ部分を前記復号部に振り分ける分岐部を有することを特徴とする請求項 1 ないし請求項 2 のいずれかに記載のデータ再生装置。

【請求項 5】 前記再生部による前記デジタルデータの先行データ部分の再生は、前記通信部によるサーバへの鍵データの要求がなされた後に行うことを特徴とする請求項 1 ないし請求項 2 のいずれかに記載のデータ再生装置。

【請求項 6】 前記デジタルデータにおける先行データ部分の所定の長さは、前記通信部によるサーバへの鍵データの要求がなされてから、前記通信部が前記サーバから送られてくる前記鍵データを受信するまでの時間より長いことを特徴とする請求項 1 ないし請求項 2 のいずれかに記載のデータ再生装置。

【請求項 7】 前記デジタルデータにおける先行データ部分と後続データ部分との間には、先行データ部分と後続データ部分とを識別する切り替え信号が挿入されていることを特徴とする請求項 1 に記載のデータ再生装置。

【請求項 8】 先頭から所定の長さ分の先行データ部分は非暗号化され、先行データ以降の後続データ部分は所定の暗号方式により暗号化され、記憶部に記憶されたデジタルデータの再生の指示を受け付ける段階と、

前記暗号方式による暗号を復号するための鍵データをサーバに要求する段階と、

前記鍵データの要求と並行して、前記デジタルデータの先行データ部分の再生を行う段階と、

前記サーバから送られてくる前記鍵データを受信する段階と、

受信した前記鍵データにより、前記デジタルデータの後続データ部分を復号する段階と、

前記デジタルデータの先行データ部分の再生後に、復号化した前記デジタルデータの後続データ部分を再生する段階とからなることを特徴とするデータ再生方法。

【請求項 9】 先頭から所定の長さ分の非暗号化された先行データ部分のみが記憶部に記憶されたデジタルデータの再生の指示を受け付ける段階と、

前記先行データ部分以降の所定の暗号方式により暗号化された後続データ部分と前記暗号方式による暗号を復号するための鍵データとをサーバに要求する段階と、

前記鍵データ及び前記デジタルデータの後続データ部分の要求と並行して、前記デジタルデータの先行データ部分の再生を行う段階と、

前記サーバから送られてくる前記鍵データと前記後続データ部分とを受信する段階と、
受信した前記鍵データにより、前記デジタルデータの後続データ部分を復号する段階と、
前記デジタルデータの先行データ部分の再生後に、復号化した前記デジタルデータの後続データ部分を再生する段階とからなることを特徴とするデータ再生方法。

【請求項 10】 前記再生部による前記デジタルデータの先行データ部分の再生は、前記通信部によるサーバへの鍵データの要求がなされた後に行うことを特徴とする請求項 8 ないし請求項 9 のいずれかに記載のデータ再生方法。

【請求項 11】 先頭から所定の長さ分の先行データ部分は非暗号化され、先行データ以降の後続データ部分は所定の暗号方式により暗号化され、記憶部に記憶されたデジタルデータの再生の指示を受け付けるステップと、前記暗号方式による暗号を復号するための鍵データをサーバに要求するステップと、
前記鍵データの要求と並行して、前記デジタルデータの先行データ部分の再生を行うステップと、
前記サーバから送られてくる前記鍵データを受信するステップと、
受信した前記鍵データにより、前記デジタルデータの後続データ部分を復号するステップと、
前記デジタルデータの先行データ部分の再生後に、復号化した前記デジタルデータの後続データ部分を再生するステップとをクライアント・コンピュータに実行させることを特徴とするデータ再生プログラム。

【請求項 12】 先頭から所定の長さ分の非暗号化された先行データ部分のみが記憶部に記憶されたデジタルデータの再生の指示を受け付けるステップと、
前記先行データ部分以降の所定の暗号方式により暗号化された後続データ部分と前記暗号方式による暗号を復号するための鍵データとをサーバに要求するステップと、
前記鍵データ及び前記デジタルデータの後続データ部分の要求と並行して、前記デジタルデータの先行データ部分の再生を行うステップと、
前記サーバから送られてくる前記鍵データと前記後続データ部分とを受信するステップと、
受信した前記鍵データにより、前記デジタルデータの後続データ部分を復号するステップと、
前記デジタルデータの先行データ部分の再生後に、復号化した前記デジタルデータの後続データ部分を再生するステップとをクライアント・コンピュータに実行させることを特徴とするデータ再生プログラム。

【請求項 13】 前記再生部による前記デジタルデータの先行部分の再生は、前記通信部によるサーバへの鍵データの要求がなされた後に行うことを特徴とする請求項 11 ないし請求項 12 のいずれかに記載のデータ再生プログラム。

【請求項 14】 先頭から所定の長さ分の先行データ部分は非暗号化され、先行データ以降の後続データ部分は所定の暗号方式により暗号化されたデジタルデータを記憶するクライアントと、

前記暗号方式による暗号を復号するための鍵データを記憶するサーバとからなるビデオ・オン・デマンド・システムであって、

前記クライアントは、

再生指示がなされたら、サーバへの鍵データの要求と、
前記デジタルデータの先行データ部分の再生とを並行して行い、

前記サーバが送信する鍵データを用いて前記デジタルデータの後続データ部分の暗号を復号化し、

前記デジタルデータの先行データ部分の再生後に、復号化した前記デジタルデータの後続データ部分を再生することを特徴とするビデオ・オン・デマンド・システム。

【請求項 15】 デジタルデータの先頭から所定の長さ分の非暗号化された先行データ部分を記憶するクライアントと、

前記先行データ部分以降の所定の暗号方式により暗号化された後続データ部分と前記暗号方式による暗号を復号するための鍵データとを記憶するサーバとからなるビデオ・オン・デマンド・システムであって、

前記クライアントは、

再生指示がなされたら、サーバへの鍵データ及び前記デジタルデータの後続データ部分の要求と、前記デジタルデータの先行データ部分の再生とを並行して行い、

前記サーバが送信する鍵データを用いて、前記サーバが送信する前記デジタルデータの後続データ部分の暗号を復号化し、

前記デジタルデータの先行データ部分の再生後に、復号化した前記デジタルデータの後続データ部分を再生することを特徴とするビデオ・オン・デマンド・システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、音声や映像等のデジタルデータを再生するためのデータ再生装置に係り、特に、暗号化されたデジタルデータを復号する鍵を入手して再生を行うデータ再生装置に関する。

【0002】

【従来の技術】音声や映像等のデジタルデータを読み出しながらその場で再生していく技術として、ストリーミング (Streaming) 技術が注目されており、例えば、ビデオ・オン・デマンド (Video On Demand) などのサービスへの応用が期待されている。

【0003】ところが、遠隔地にあるサーバからデジタルデータを読み出しながらその場で再生していくためには、高速・高品位の回線が必要となるため、通常は各種方式の符号化 (データ圧縮) 技術を用いてデータを圧縮したりして、伝送量を削減したりしている。

【0004】また、音声や映像等のデジタルデータを、各種方式の暗号化技術を用いて暗号化し、それをCD-ROM (Compact Disc Read Only Memory) やDVD-ROM (Digital Versatile Disc Read Only Memory) 等の記録媒体に記録して、予め利用者に配布するといった形態のビデオ・オン・デマンド・システムもあり、図11は、このような従来のビデオ・オン・デマンドシステムを例示する概略構成図である。

【0005】予め、配布された記録媒体の暗号化されたビデオデータは、データ再生装置としてのクライアント400内の記憶部404に転送され記憶されている。

【0006】ビデオ・オン・デマンドの利用者は、クライアント400の入力部401からビデオデータの再生の指示を行う。この指示を受けた制御部402は、サーバ200に対して再生するビデオデータの暗号を解く（復号する）ための鍵データを要求するように、通信部404を制御する。

【0007】通信網300を経由して、クライアント400からの鍵データの要求を受信したサーバ200の制御部202は、記憶部201内に記憶している鍵データをクライアント400に返送するように、通信部203を制御する。

【0008】通信網300を経由して、サーバ200からの鍵データを受信したクライアント400は、記憶部404からビデオデータを順次読み出し、読み出したビデオデータの暗号を復号部405にて鍵データを用いて解読し、解読したビデオデータを再生部407にて順次再生する。

【0009】このように、予め暗号化されたビデオデータをクライアント400側に配布しておき、サーバ200からは鍵データのみを伝送することで、たとえ通信網300の回線が高速でなくても、ストリーミング再生を行うことができる。

【0010】

【発明が解決しようとする課題】しかしながら、上記の如きビデオ・オン・デマンド・システムでは、以下のような問題があった。

【0011】一般に、通信網を用いた通信路の確立には、相応の時間を要する。従って、図12に例示するように、クライアントがサーバに対して鍵データの要求を行ってから、サーバから鍵データが送られてくるまでの時間 t_2 が長くなると、利用者が再生の指示をしてから実際にデジタルデータ10の再生が開始されるまでの時間（アクセス時間） t_1 も長くなる。つまり、利用者が再生の指示を出しても、即座に再生が開始されないことになり、利用者にストレスを感じさせてしまう。

【0012】本発明は、上述の如き従来の問題点を解決するためになされたものであり、利用者が再生の指示をしてから実際にデジタルデータの再生が開始されるまでの時間（アクセス時間）を短縮し、即座にデジタルデー

タの再生を開始することのできるデータ再生装置、データ再生方法、データ再生プログラム、およびビデオ・オン・デマンド・システムを提供することを目的とする。

【0013】

【課題を解決するための手段】上記目的を達成するために、本発明は、文字、音声、静止画像、動画像、等々の情報をデジタル信号化したデジタルデータの、先行データ部分は非暗号とし、後続データ部分にのみ暗号化を施して、クライアントに配布しておき、クライアントは、再生指示がなされたら、サーバへの暗号を解くための鍵データの要求とデジタルデータの先行データ部分の再生とを並行して行うことで、サーバから鍵データが送られてくるまでの間は、非暗号の先行データ部分の再生を先行して行い、サーバから鍵データが送られてきたら、暗号化された後続データ部分の復号化を行いながら、先行データ部分の再生に続いて後続データ部分の再生を行うことができる。つまり、サーバからの鍵データの応答時間に依存することなく、先行データ部分の再生を先行して行うことができるため、利用者が再生の指示をしてから実際にデジタルデータの再生が開始されるまでの時間（アクセス時間）を大幅に短縮することができる。

【0014】「サーバへの鍵データの要求」と「デジタルデータの先行部分の再生」とは同時に行っても良いし、どちらか一方を先に他方を後に行っても良いが、利用者が再生の指示をしてから実際にデジタルデータの再生が開始されるまでの時間（アクセス時間）の短縮を優先するのであれば、「サーバへの鍵データの要求」よりも「デジタルデータの先行部分の再生」の方を先に行う、あるいは両者を同時に行うようにすべきである。

【0015】また、デジタルデータにおける先行データ部分の所定の長さは、サーバへの鍵データの要求がなされてから鍵データが送られてくるまでに必要な時間にしておくべきである。

【0016】また、本発明は、サーバからデジタルデータを読み出しながら再生する形態にも適用することができる。つまり、デジタルデータの先頭から所定の長さ分の非暗号化された先行データ部分をクライアント側に、先行データ部分以降の所定の暗号方式により暗号化された後続データ部分と鍵データとをサーバ側に記憶させておき、クライアントは、再生指示がなされたら、サーバへの鍵データ及びデジタルデータの後続データ部分の要求と、デジタルデータの先行データ部分の再生とを並行して行うことで、サーバから鍵データが送られてくるまでの間は、非暗号の先行データ部分の再生を先行して行い、サーバから鍵データが送られてきたら、サーバから送られてくる後続データ部分の復号化を行いながら、先行データ部分の再生に続いて後続データ部分の再生を行うことができる。

【0017】また、クライアント側の装置は、データ再生専用のハードウェアとしても実現可能であるが、デー

タ再生装置の構成要素の全部もしくは一部をソフトウェアによって構成し、それをパーソナルコンピュータ等で実行することで実現することも可能である。

【0018】

【発明の実施の形態】以下、本発明の実施形態を図面に基づいて説明する。

【0019】〔第1の実施の形態〕図1は、本実施形態におけるビデオ・オン・デマンド・システムの一例を示す概略構成図である。

【0020】データ再生装置としてのクライアント100は、デジタルデータの再生の要求を受け付ける入力部101、後述する処理手順に従ってクライアント100を構成する各部の制御を行う制御部102、通信網300を介してサーバ200に対して通信を行う通信部103、音声や映像等のデジタルデータが予め記憶されている記憶部104、デジタルデータにかけられている暗号を解除する復号部105、記憶部に記憶されているデジタルデータと復号部にて復号化されるデジタルデータとを順次再生部107に送る多重部106、デジタルデータを再生・出力する再生部107などから構成されている。尚、後述する処理手順は、データ再生装置としてクライアント100を構成するコンピュータ等が実行可能なデータ再生プログラムとして各種記録メディアに格納し、または通信メディアにより伝送して、頒布することができる。クライアント100の制御部102は、上記データ再生プログラムに記述された処理手続きに従って上記各部の処理制御を実行する。

【0021】サーバ200は、デジタルデータにかけられている暗号を解除するための鍵データを記憶する記憶部201、サーバ200を構成する各部の制御を行う制御部202、通信網300を介してクライアント100に対して通信を行う通信部203などから構成されている。

【0022】音声や映像等のデジタルデータは、CD-ROMやDVD-ROMといった記録媒体に記録されて予め利用者のもとに配布され、配布されたデジタルデータは、クライアント100内の記憶部104に転送され記憶されている。尚、デジタルデータの配布の方法はこれに限定されず、例えば、通信網300などの伝送媒体を介してクライアント100内の記憶部104に転送するようにしても良い。

【0023】図2は、利用者に配布されるデジタルデータの構造を模式化した図である。同図(a)は従来のビデオ・オン・デマンド・システムにて利用者に配布されるデジタルデータの状態を示しており、データ10全体に対して暗号化が施されている。それに対して、同図

(b)は本実施形態において利用者に配布されるデジタルデータの状態を示しており、先頭から所定の長さ分の先行データ部分10aは暗号化されておらず、先行データ部分10a以降の後続データ部分10bは、所定の暗

号方式により予め暗号化された状態で、利用者に配布されクライアント100内記憶部104に記憶される。先行データ部分の所定の長さは、サーバへの鍵データの要求がなされてから鍵データが送られてくるまでに必要な時間になるように時間配分がなされている。

【0024】また、同図(c)は、先行データ部分10aの先頭に非暗号化開始信号11、先行データ部分10aと後続データ部分10bとの間に暗号化開始信号12を挿入した例を示している。

【0025】次に、以上のように構成された本実施形態における処理動作について、図3に例示するタイムチャート及び図4に例示するフローチャートに基づいて説明する。

【0026】まず、クライアント100の入力部101にて利用者によるデジタルデータの再生要求信号を受け付ける(Step01)。

【0027】受け付けた再生要求信号を契機に、クライアント100は以下の処理(a)、(b)を並行して行う。

【0028】(a)制御部102は、ビデオデータ後続データ部分10bの暗号を復号するための鍵データをサーバ200に要求するように、通信部103を制御する。通信部103は、通信網300を介してサーバ200に鍵データ要求信号を送る(Step02)。

【0029】(b)制御部102は、多重部106に読み出し開始信号を送り、多重部106は、記憶部104に記憶されているデジタルデータの先行データ部分10aの読み出しを開始する。多重部106は、読み出したデジタルデータの先行データ部分10aを順次再生部107へ送る(Step03)。再生部107は、送られてきた先行データ部分10aを再生・出力する(Step04)。

【0030】この際、デジタルデータの先行データ部分10aには暗号が施されていないため、鍵データがなくても、再生部107は先行データ部分10aの再生が可能である。

【0031】多重部106は、記憶部104から先行データ部分10aの読み出しを開始してからの経過時間を計測しており、所定の時間(t3)が経過したかどうか判定する。この所定の時間(t3)は、デジタルデータの先行データ部分10aとして確保した長さに対応しており、所定の時間(t3)が経過するまでは、Step03～Step04の処理を繰り返す(Step05)。

【0032】この間に、サーバ200の制御部202は、通信網300を介して通信部203がクライアント100から受信した鍵データの要求を受け付け、記憶部201内の鍵データを読み出す。そして、読み出した鍵データを通信部203がクライアント100宛に送信する。

【0033】クライアント100の制御部102は、通信部103が鍵データを受信したことを確認すると(St

ep06)、受信した鍵データを復号部105へ格納し、復号開始信号を復号部105へ送る。

【0034】復号部105は、鍵データを用いて、記憶部104に記憶されているデジタルデータの後続データ部分10bを読み出して暗号を解除し、多重部106へ送る(Step08)。

【0035】多重部106は、復号済みの後続データ部分10bを、先行データ部分10aに引き続いて、再生部107に順次送り、再生部107はこれを再生・出力する(Step09)。後続データ部分10bの処理が全て終了するまで、Step07~Step09の各処理を繰り返す(Step10)。

【0036】このように、利用者から再生指示がなされたら、サーバ200への暗号を解くための鍵データの要求とデジタルデータの先行データ部分10aの再生とを並行して行うことで、サーバ200から鍵データが送られてくるまでの間は、非暗号の先行データ部分10aの再生を先行して行い、サーバ200から鍵データが送られてきたら、暗号化された後続データ部分10bの復号化を行いながら、先行データ部分10aの再生に続いて後続データ部分10bの再生を行うことができる。これにより、サーバ200からの鍵データの応答時間(t2)に依存することなく、先行データ部分10aの再生を先行して行うことができるため、利用者が再生の指示をしてから実際にデジタルデータの再生が開始されるまでのアクセス時間(t1)を大幅に短縮することができる。

【0037】〔第2の実施の形態〕第1の実施形態では、「サーバへの鍵データの要求」と「デジタルデータの先行部分の再生」とを同時に並行して行う例を示した。利用者が再生の指示をしてから実際にデジタルデータの再生が開始されるまでの時間(アクセス時間)の短縮を優先するのであれば、「サーバへの鍵データの要求」よりも「デジタルデータの先行部分の再生」の方を先に行う、あるいは両者を同時に行うようにすべきである。

【0038】そこで、本実施の形態では、「サーバへの鍵データの要求」を行った後に「デジタルデータの先行部分の再生」を行う例を、図4のフローチャートに示す。

【0039】クライアント100の入力部101にて利用者によるデジタルデータの再生要求信号を受け付けた(Step01)後に、まず、制御部102が、ビデオデータ後続データ部分10bの暗号を復号するための鍵データをサーバ200に要求するように、通信部103を制御する。通信部103は、通信網300を介してサーバ200に鍵データ要求信号を送る(Step02)。

【0040】その後、制御部102は、多重部106に読み出し開始信号を送り、多重部106は、記憶部104に記憶されているデジタルデータの先行データ部分1

0aの読み出しを開始する。多重部106は、読み出したデジタルデータの先行データ部分10aを順次再生部107へ送る(Step03)。再生部107は、送られてきた先行データ部分10aを再生・出力する(Step04)。

【0041】Step05以降の処理の流れは、図4のフローチャートを用いて説明した第1の実施形態における処理手順と同様である。

【0042】〔第3の実施の形態〕第1、第2の実施形態では、クライアント100の多重部106が、デジタルデータの先行データ部分10aとして確保した長さに対応した、所定の時間(t3)に基づいて、先行データ部分10aと後続データ部分10bとの処理の切り替えを行う例を示した。

【0043】本実施の形態では、図2(c)に示したように、デジタルデータの先行データ部分10aと後続データ部分10bとの間に暗号化開始信号12を予め挿入しておき、クライアント100の多重部106は、この信号により先行データ部分10aと後続データ部分10bとの処理の切り替えを行う例を示す。

【0044】図6は、本実施形態における処理動作を例示したフローチャートである。

【0045】まず、クライアント100の入力部101にて利用者によるデジタルデータの再生要求信号を受け付ける(Step21)。

【0046】次に、クライアント100の制御部102は、ビデオデータ後続データ部分10bの暗号を復号するための鍵データをサーバ200に要求するように、通信部103を制御し、通信部103は、通信網300を介してサーバ200に鍵データ要求信号を送る(Step22)。

【0047】その後、制御部102は、多重部106に読み出し開始信号を送り、多重部106は、記憶部104に記憶されているデジタルデータの先行データ部分10aの読み出しを開始する(Step23)。

【0048】ここで、多重部106は、読み出したデジタルデータが暗号化開始信号12であるかどうか判定し(Step24)、暗号化開始信号12でない場合には、まだ先行データ部分10aを読み出し中であると認識して、読み出した先行データ部分10aを再生部へ送る。再生部107は、送られてきた先行データ部分10aを再生・出力する(Step25)。

【0049】Step24にて、読み出したデータが暗号化開始信号12である場合には、先行データ部分10aが終了し、後続データ部分10bに切り替わると認識して、以降、後続データ部分10bに対応した処理を行う。Step26以降は、図4、5に示したStep06以降の処理と同様である。

【0050】尚、本実施の形態では、第2の実施形態と同様に、「サーバへの鍵データの要求」を行った後に「デジタルデータの先行部分の再生」を行う処理手順を

モデルに説明したが、第1の実施の形態と同様に、「サーバへの鍵データの要求」よりも「デジタルデータの先行部分の再生」の方を先に行う、あるいは両者を同時に行う処理手順にも適用することができる。

【0051】尚、図7に示すように、クライアント100内に分岐部108を配置して、この分岐部108が、記憶部104から読出したデジタルデータを判定して処理を分岐させるようにしても良い。つまり、分岐部108は、記憶部104から読み出したデジタルデータが先行データ部分10aである場合には、当該データをそのまま再生部107に送る。逆に、読み出したデジタルデータが後続データ部分10bである場合には、当該データを復号部105へ送って復号化処理を施すような処理形態にしても良い。

【0052】〔第4の実施の形態〕第1～第3の実施形態では、音声や映像等のデジタルデータを予め利用者のもとに配布して、クライアント100内の記憶部104に記憶しておく形態を説明したが、本発明に係る技術的思想は、サーバ200からデジタルデータを読み出しながら再生する形態にも適用することができる。

【0053】図8は、本実施形態におけるビデオ・オン・デマンド・システムの一例を示す概略構成図である。デジタルデータの先頭から所定の長さ分の非暗号化された先行データ部分10aのみを予め利用者に配布し、クライアント側にクライアント100内の記憶部104に記憶しておく。また、デジタルデータのうち、所定の暗号方式により暗号化された後続データ部分10bと鍵データとをサーバ200側の記憶部201に予め記憶させておく。

【0054】次に、本実施形態における処理動作について、図9に例示するタイムチャート及び図10に例示するフローチャートに基づいて説明する。

【0055】まず、クライアント100の入力部101にて利用者によるデジタルデータの再生要求信号を受け付ける(Step41)。

【0056】受け付けた再生要求信号を契機に、クライアント100は以下の処理(a)、(b)を並行して行う。

【0057】(a)制御部102は、鍵データ及びデジタルデータの後続データ部分10bをサーバ200に要求するように、通信部103を制御する。通信部103は、通信網300を介して、サーバ200に鍵データ及びデジタルデータの後続データ部分10bの要求信号を送る(Step42)。

【0058】(b)制御部102は、再生部107に読み出し開始信号を送り、再生部107は、記憶部104に記憶されているデジタルデータの先行データ部分10aの読み出しを開始し(Step43)、それを順次再生・出力する(Step44)。

【0059】再生部107は、所定の時間(t3)が経

過するまでは、Step43～Step44の処理を繰り返す(Step45)。

【0060】この間に、サーバ200の制御部202は、通信網300を介して通信部203がクライアント100から受信した鍵データ及び後続データ部分10bの要求を受け付け、記憶部201内の鍵データ及びデジタルデータの後続データ部分10bを読み出してクライアント100宛に送信する。

【0061】クライアント100の制御部102は、通信部103が鍵データ及びデジタルデータの後続データ部分10bを受信したことを確認すると(Step46)、受信した鍵データを復号部105へ格納し、復号開始信号を復号部105へ送る。

【0062】復号部105は、鍵データを用いて、通信部103が受信したデジタルデータの後続データ部分10bを読み出して暗号を解除し、再生部107へ送る

(Step48)。再生部107はこれを再生・出力し(Step49)、後続データ部分10bの処理が全て終了するまで、Step47～Step49の各処理を繰り返す(Step50)。

【0063】このように、サーバ200からデジタルデータを読み出しながらストリーミング再生する形態においても、サーバ200からの鍵データ及び後続データ部分10bの応答時間(t2)に依存することなく、利用者が再生の指示をしてから実際にデジタルデータの再生が開始されるまでのアクセス時間(t1)を大幅に短縮することができる。

【0064】本実施形態にて説明した方式は、予め、デジタルデータの先行データ部分10aのみを利用者のクライアント100に配布しておくだけで良く、後続データ10bを含む全てのデジタルデータを配布する必要がないため、記憶部104の記憶容量が比較的小さな、例えば、携帯電話やPDA(Personal Digital Assistant)といった携帯型情報端末をクライアント100とするのに好適である。

【0065】以上、本発明について第1～第4の実施形態にて詳細に説明したが、本発明は本実施形態に限定されず、本発明の主旨を逸脱しない範囲において、種々の改良や変更を成し得るであろう。

【0066】

【発明の効果】以上説明したように、利用者から再生指示がなされたら、サーバへの暗号を解くための鍵データの要求とデジタルデータの先行データ部分の再生とを並行して行うことで、サーバから鍵データが送られてくるまでの間は、非暗号の先行データ部分の再生を先行して行い、サーバから鍵データが送られてきたら、暗号化された後続データ部分の復号化を行いながら、先行データ部分の再生に続いて後続データ部分の再生を行うことができる。これにより、サーバからの鍵データの応答時間に依存することなく、先行データ部分の再生を先行して行うことができるため、利用者が再生の指示をしてから

実際にデジタルデータの再生が開始されるまでの時間（アクセス時間）を大幅に短縮することができる。

【0067】また、サーバからデジタルデータを読み出しながらストリーミング再生する形態においても、サーバからの鍵データ及び後続データ部分の応答時間に依存することなく、利用者が再生の指示をしてから実際にデジタルデータの再生が開始されるまでの時間（アクセス時間）を大幅に短縮することができる。

【図面の簡単な説明】

【図1】本発明における第1の実施形態に係るビデオ・オン・デマンド・システムの構成を示す概略構成図である。

【図2】図1に示したビデオ・オン・デマンド・システムに用いられるデジタルデータの構成を模式化したイメージ図である。

【図3】図1に示したビデオ・オン・デマンド・システムにおけるクライアントの処理動作のタイミングを示すタイミングチャートである。

【図4】図1に示したビデオ・オン・デマンド・システムにおけるクライアントの処理動作手順を示すフローチャートである。

【図5】本発明における第2の実施形態に係るクライアントの処理動作手順を示すフローチャートである。

【図6】本発明における第3の実施形態に係るクライアントの処理動作手順を示すフローチャートである。

【図7】本発明における第3の実施形態に係るビデオ・オン・デマンド・システムの構成を示す概略構成図である。

【図8】本発明における第4の実施形態に係るビデオ・オン・デマンド・システムの構成を示す概略構成図であ

る。

【図9】図8に示したビデオ・オン・デマンド・システムにおけるクライアントの処理動作のタイミングを示すタイミングチャートである。

【図10】図8に示したビデオ・オン・デマンド・システムにおけるクライアントの処理動作手順を示すフローチャートである。

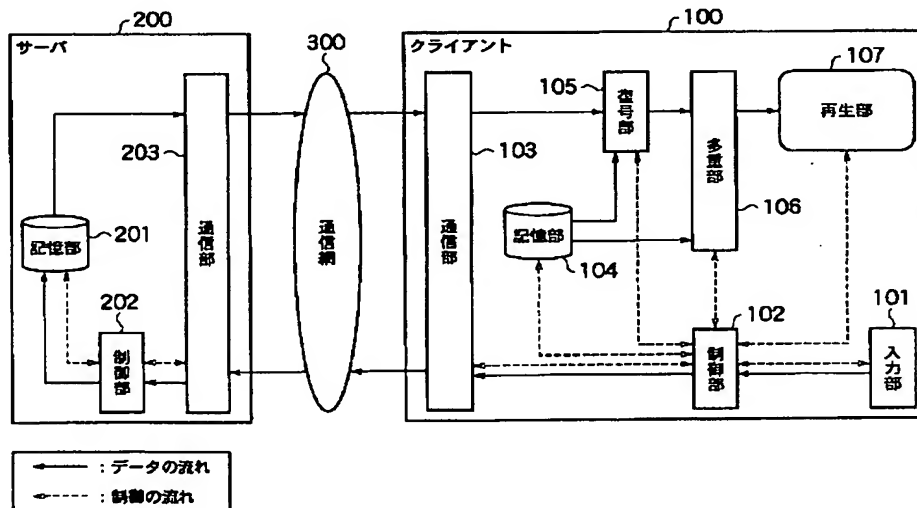
【図11】従来のビデオ・オン・デマンド・システムの構成を示す概略構成図である。

【図12】図11に示した従来のビデオ・オン・デマンド・システムにおけるクライアントの処理動作手順を示すフローチャートである。

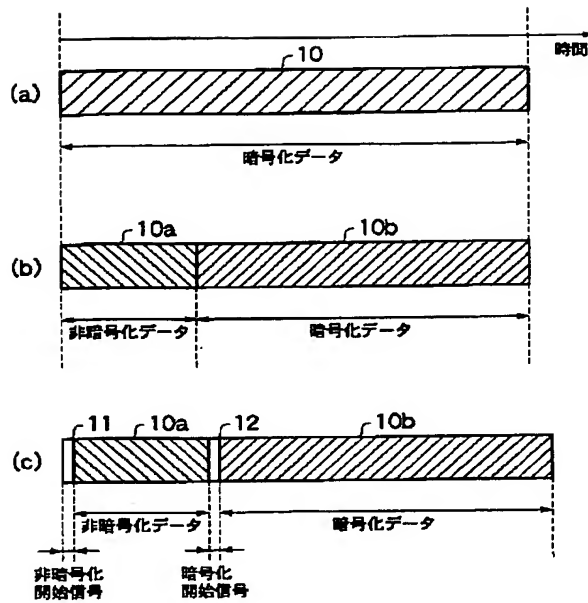
【符号の説明】

- 10...デジタルデータ
- 10a...先行データ部分
- 10b...後続データ部分
- 100...クライアント（データ再生装置）
- 101...入力部
- 102...制御部
- 103...通信部
- 104...記憶部
- 105...復号部
- 106...多重部
- 107...再生部
- 200...サーバ
- 201...記憶部
- 202...制御部
- 203...通信部
- 300...通信網

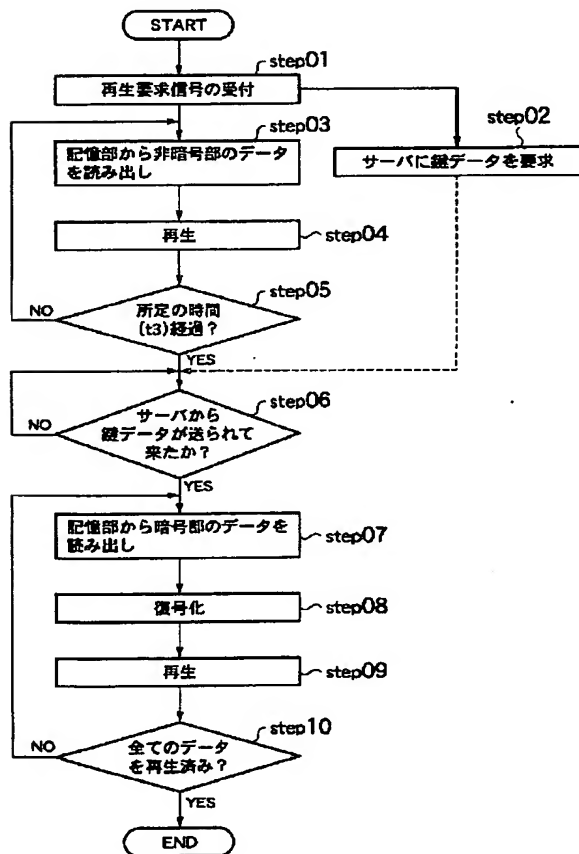
【図1】



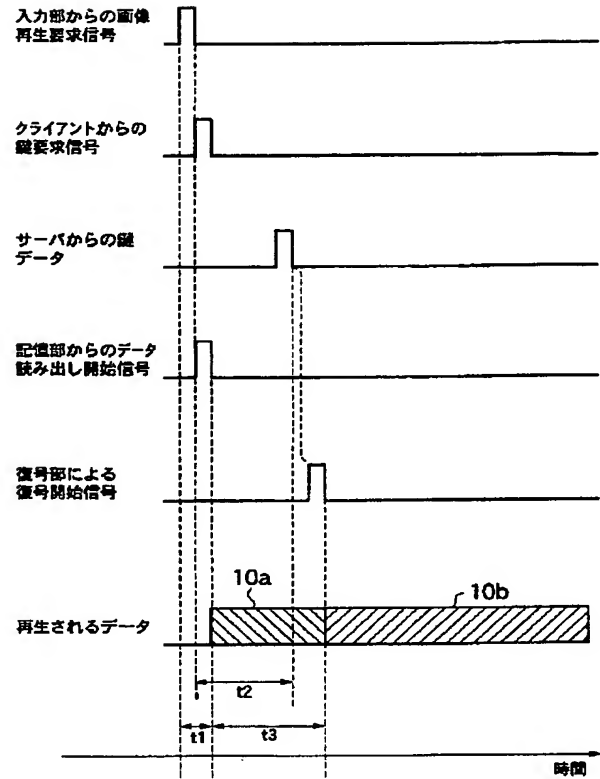
【図2】



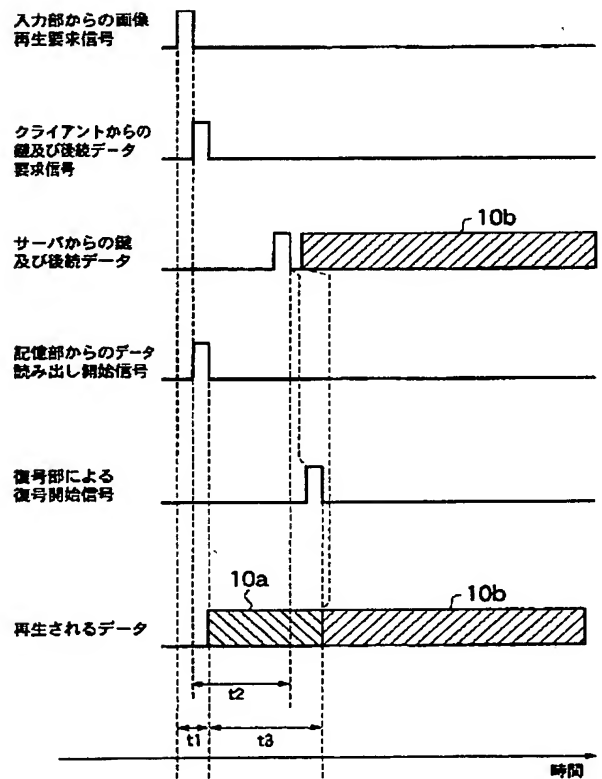
【図4】



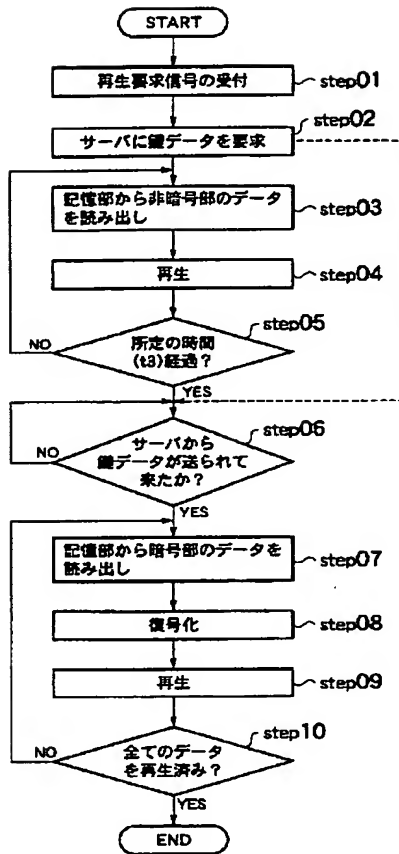
【図3】



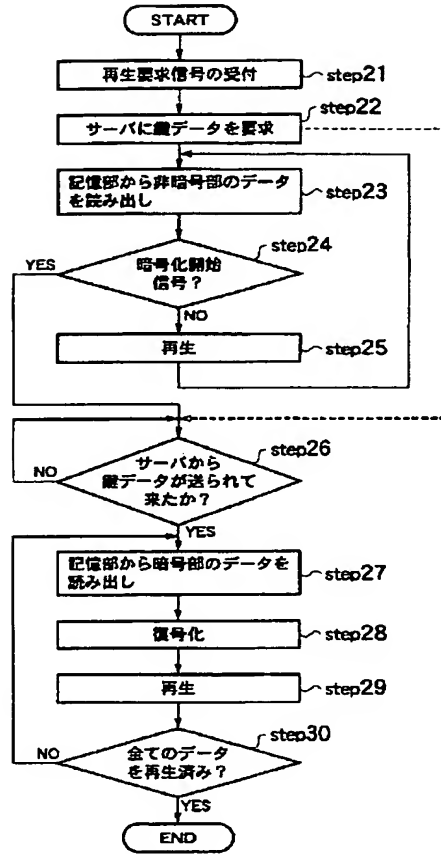
【図9】



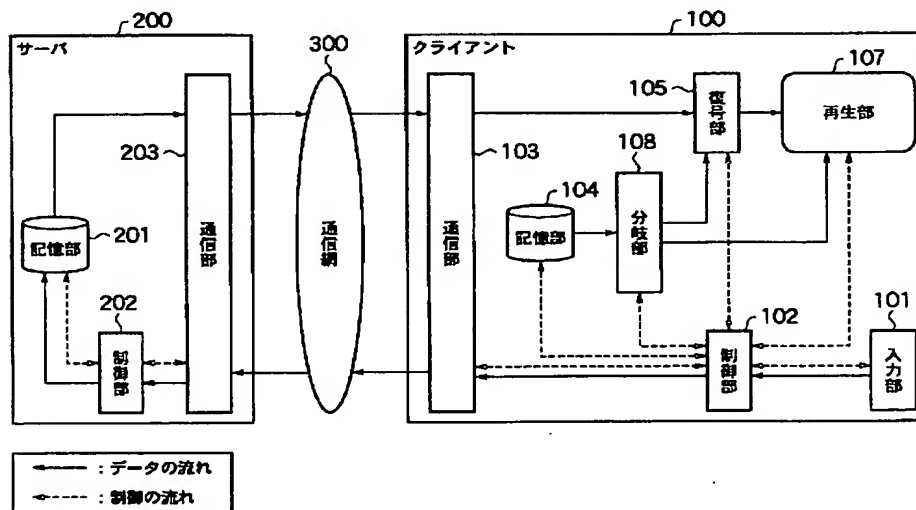
【図5】



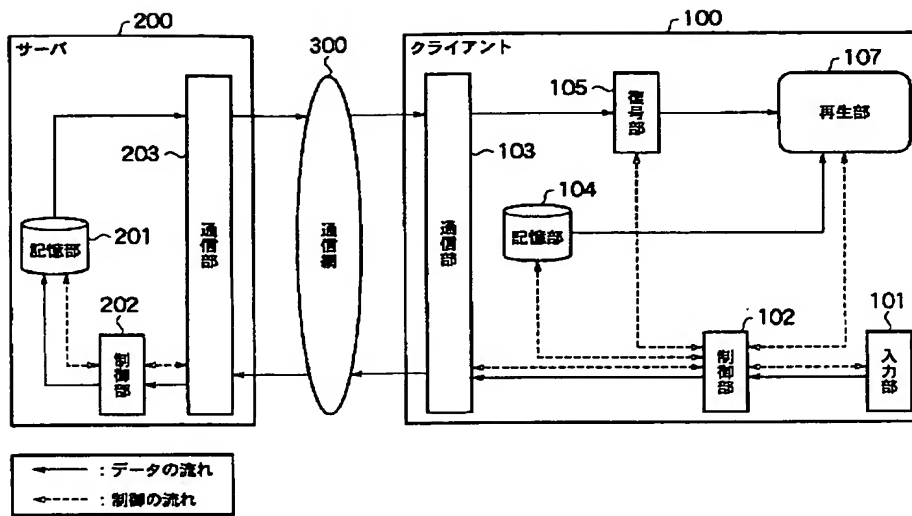
【図6】



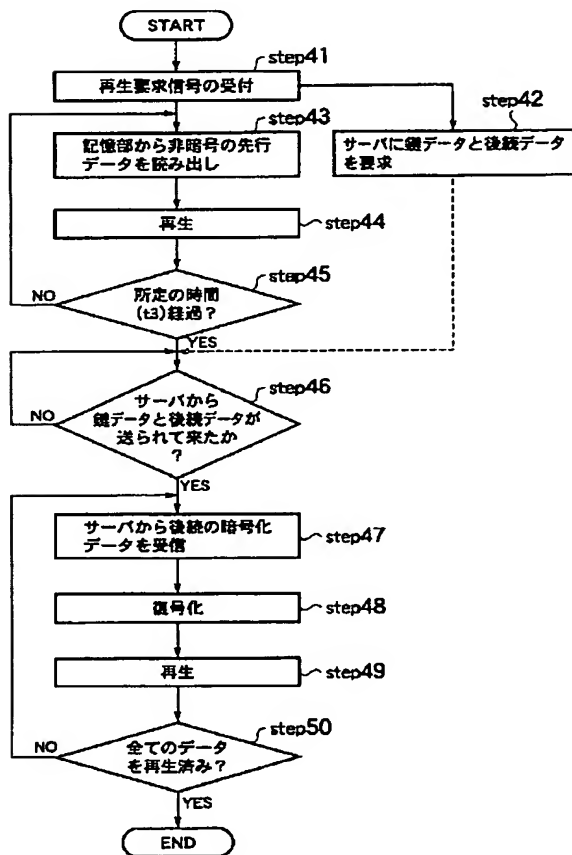
【図7】



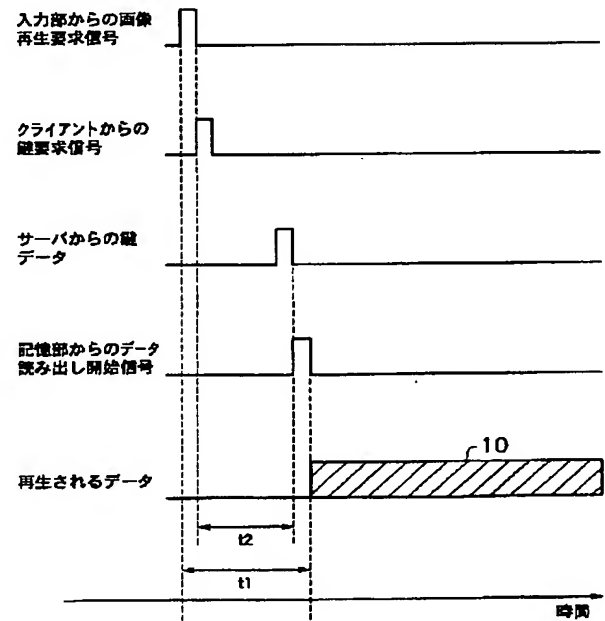
【図8】



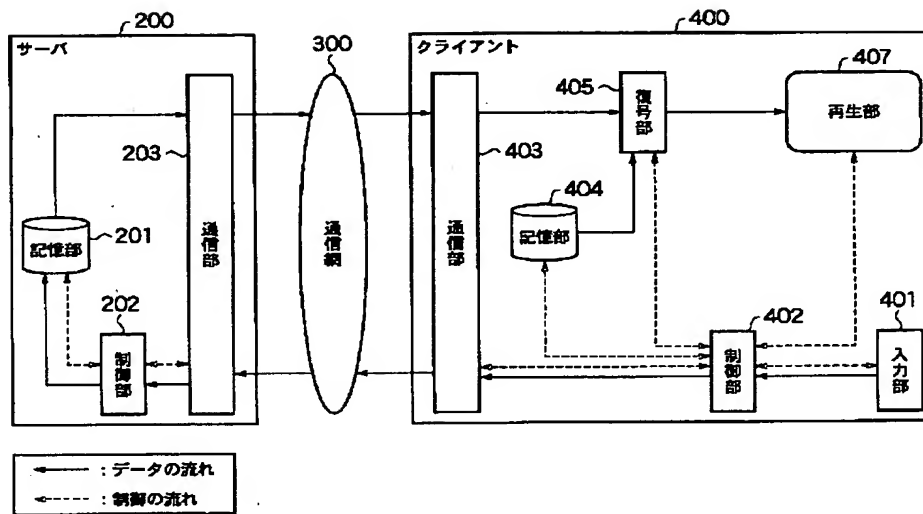
【図10】



【図12】



【図11】



フロントページの続き

(51) Int. Cl.⁷

H 0 4 N 7/173

識別記号

6 3 0

F I

H 0 4 L 9/00

テームコード* (参考)

6 4 3

F ターム (参考) 5C053 FA30 GB06 GB40 JA03 JA21

KA24 LA14

5C064 BA01 BA07 BB05 BB10 BC06

BC10 BC17 BC20 BC25 BD02

BD09 CB01 CC04

5D044 AB05 AB07 AB09 DE02 DE03

DE12 DE92 DE96 FG23 GK12

GK17

5J104 AA01 AA16 AA33 EA04 EA15

NA02 PA14